DMARC Adoption in the UAE: 2023 Report

POWERDMARC

POWERDMARC

Case study

DMARC Adoption in the UAE: 2023 Report

- DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol designed to give email domain owners the ability to protect their domain from unauthorized use, or "spoofing". Email authentication is important because it helps to prevent spam and phishing attacks that can harm both individuals and businesses. These attacks can use a fake email address that appears to come from a legitimate source to trick recipients into disclosing sensitive information or downloading ransomware.
- In addition to improving email security, DMARC also provides reporting features that allow domain owners to receive feedback about email traffic sent from their domain. This helps organizations to identify and address any issues related to email delivery, and to improve their email authentication policies over time.

Assessing the Threat Landscape

- Like any other country, the United Arab Emirates (UAE) is vulnerable to email phishing and spoofing attacks. These types of attacks are not specific to any particular region or country but rather are global cybersecurity threat that affects individuals and organizations worldwide.
- The UAE is home to many large corporations and financial institutions that are attractive targets for cybercriminals. Furthermore, the country's population is highly connected and reliant on technology, making them more susceptible to phishing and spoofing attacks. To combat these threats, the UAE has implemented various measures to enhance cybersecurity, which work to protect the country's critical infrastructure and provide support to individuals and organizations. However, it is still important for individuals and organizations to take proactive measures to protect themselves against these types of attacks, such as increasing the DMARC and email authentication adoption rate in the country.

In our UAE DMARC Adoption Report for 2023, we will address the following major concerns:

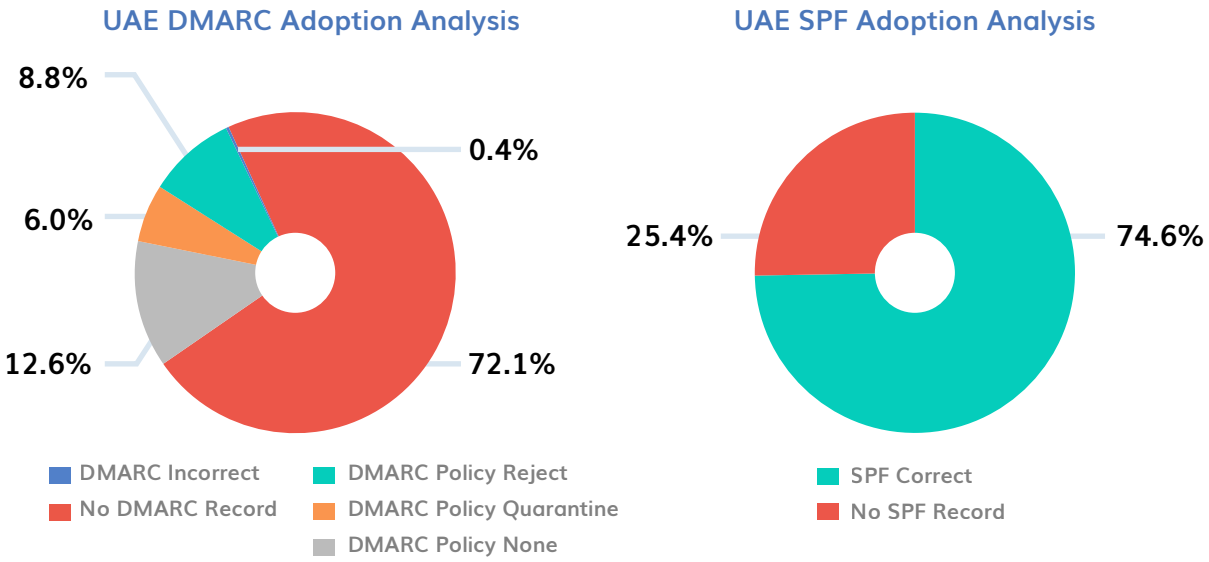
- What is the current situation of DMARC adoption and enforcement in organizations in the UAE?
- How can we improve the cybersecurity and email authentication infrastructure in the UAE to mitigate impersonation attacks?

To gain better insight into the current scenario we analyzed 961 domains belonging to top businesses and organizations in the UAE, from the following sectors:

- Banking
- Government
- Healthcare
- Energy
- Telecommunications
- Education
- Transport
- Media and Entertainment

What Do the Numbers Say?

An in-depth SPF and DMARC adoption analysis was conducted while examining all 961 UAE domains, which led to the following revelations:



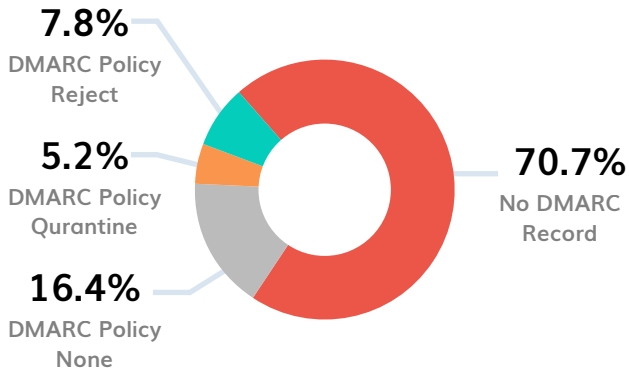
- Graphical Analysis: Among all 961 domains examined that belong to various organizations in the UAE, 660 domains (68.7%) possessed correct SPF records, while 225 domains (23.4%) unfortunately had no SPF records at all. 264 domains (27.5%) had correct DMARC records, while 4 of the domains (0.4%) had DMARC records that contained errors. A vast majority of domains (693 domains making up 72.1%) had no DMARC records at all. 121 domains had their DMARC policy set at none (12.6%), enabling monitoring only, while 58 domains (6.03%) had their DMARC policy level set at quarantine, and 85 domains (8.8%) had their DMARC policy set at maximum enforcement (i.e. p=reject)

Sector-wise Analysis of UAE Domains

Healthcare Sector

UAE SPF Adoption Analysis in the Healthcare Sector

UAE DMARC Adoption Analysis in the Healthcare Sector



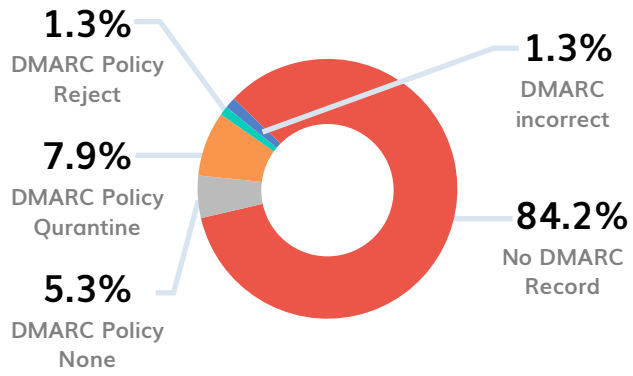
Key Findings:

- 23.1% of domains had no SPF record
- 16.4% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 70.7% of the domains

Energy Sector

UAE SPF Adoption Analysis in the Energy Sector

UAE DMARC Adoption Analysis in the Energy Sector

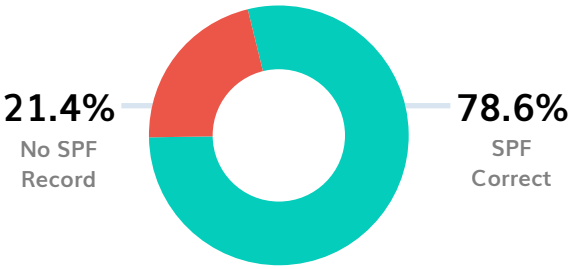


Key Findings:

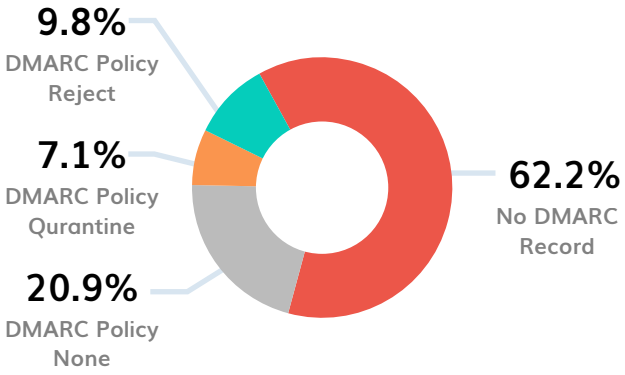
- 27.5% of domains had no SPF record
- 5.3% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 84.2% of the domains

Government Sector

UAE SPF Adoption Analysis in the Government Sector



UAE DMARC Adoption Analysis in the Government Sector

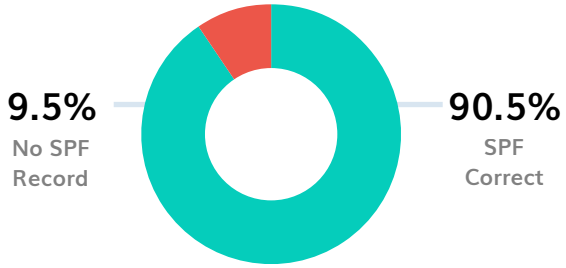


Key Findings:

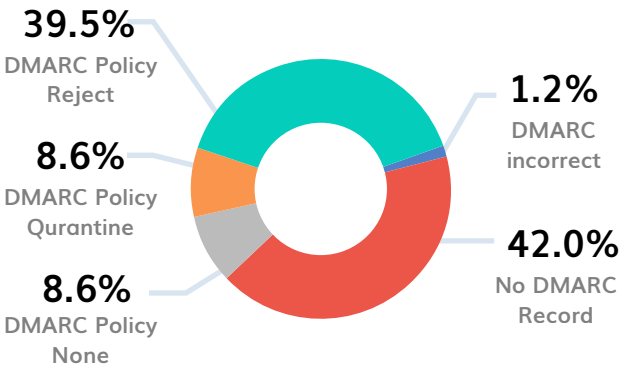
- 21.4% of domains had no SPF record
- 20.9% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 62.2% of the domains

Banking Sector

UAE SPF Adoption Analysis in the Banking Sector



UAE DMARC Adoption Analysis in the Banking Sector



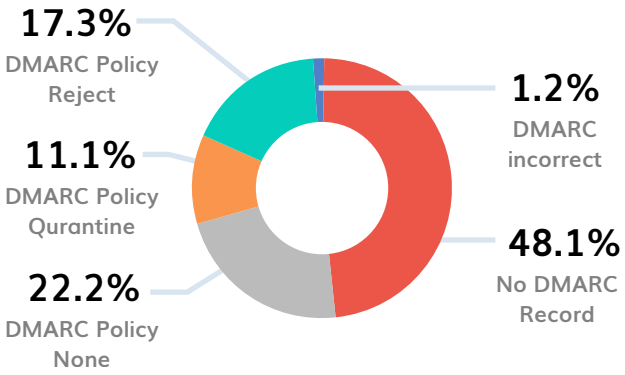
Key Findings:

- 9.5% of domains had no SPF record
- 8.6% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 42% of the domains

Education Sector

UAE SPF Adoption Analysis in the Education Sector

UAE DMARC Adoption Analysis in the Education Sector



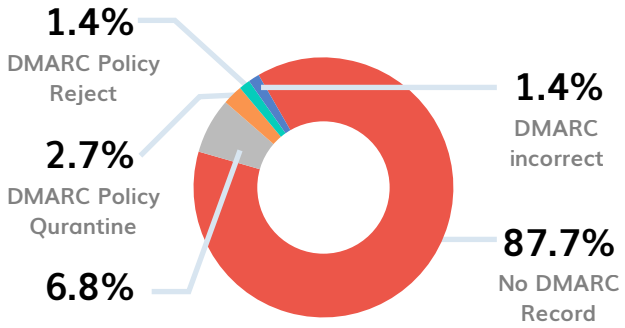
Key Findings:

- 26.4% of domains had no SPF record
- 22.2% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 48.1% of the domains

Telecom Sector

UAE SPF Adoption Analysis in the Telecom Sector

UAE DMARC Adoption Analysis in the Telecom Sector



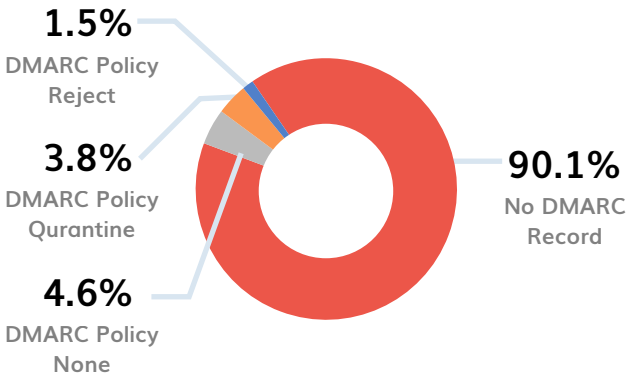
Key Findings:

- 35.3% of domains had no SPF record
- 6.8% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 87.7% of the domains

Media and Entertainment Sector

UAE SPF Adoption Analysis in the Media and Entertainment Sector

UAE DMARC Adoption Analysis in the Media and Entertainment Sector



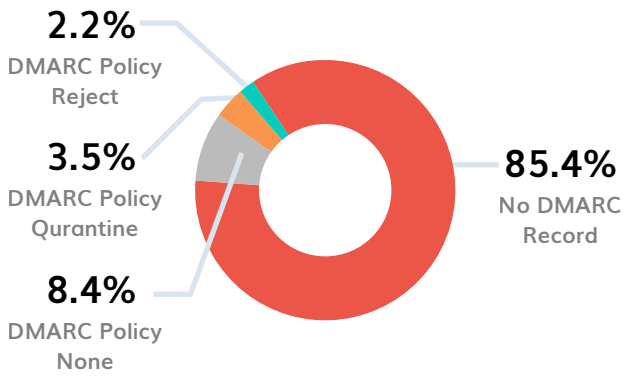
Key Findings:

- 37.6% of domains had no SPF record
- 4.6% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 90.1% of the domains

Transport Sector

UAE SPF Adoption Analysis in the Transport Sector

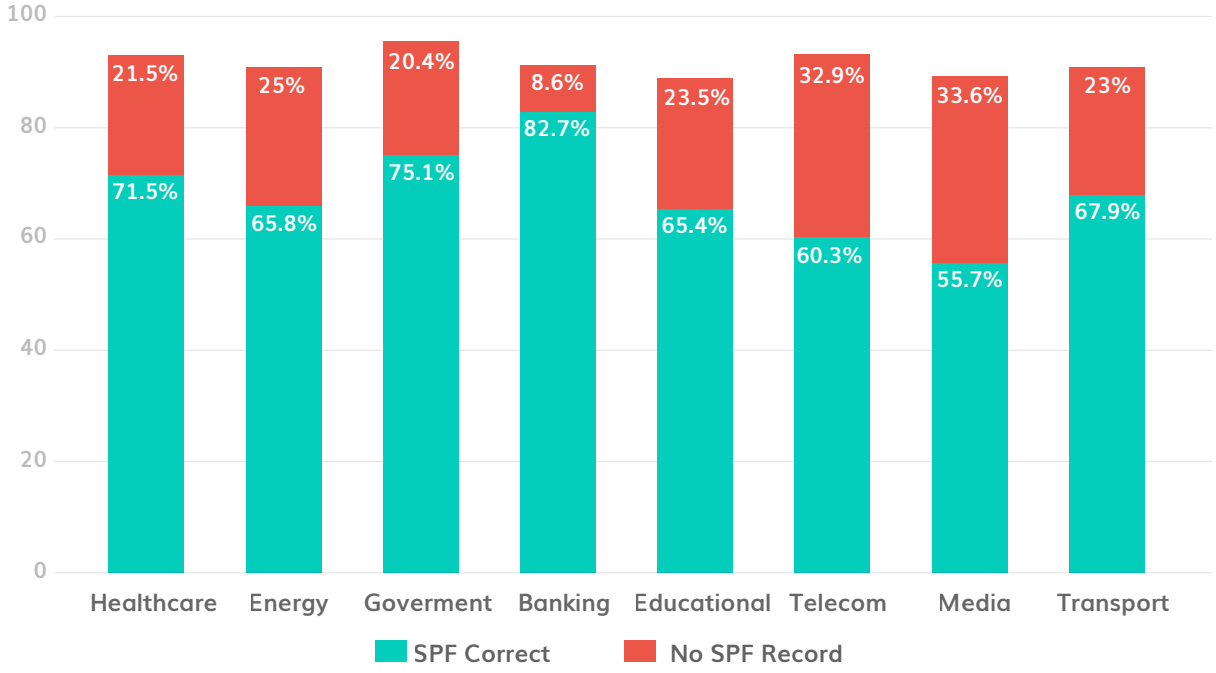
UAE DMARC Adoption Analysis in the Transport Sector



Key Findings:

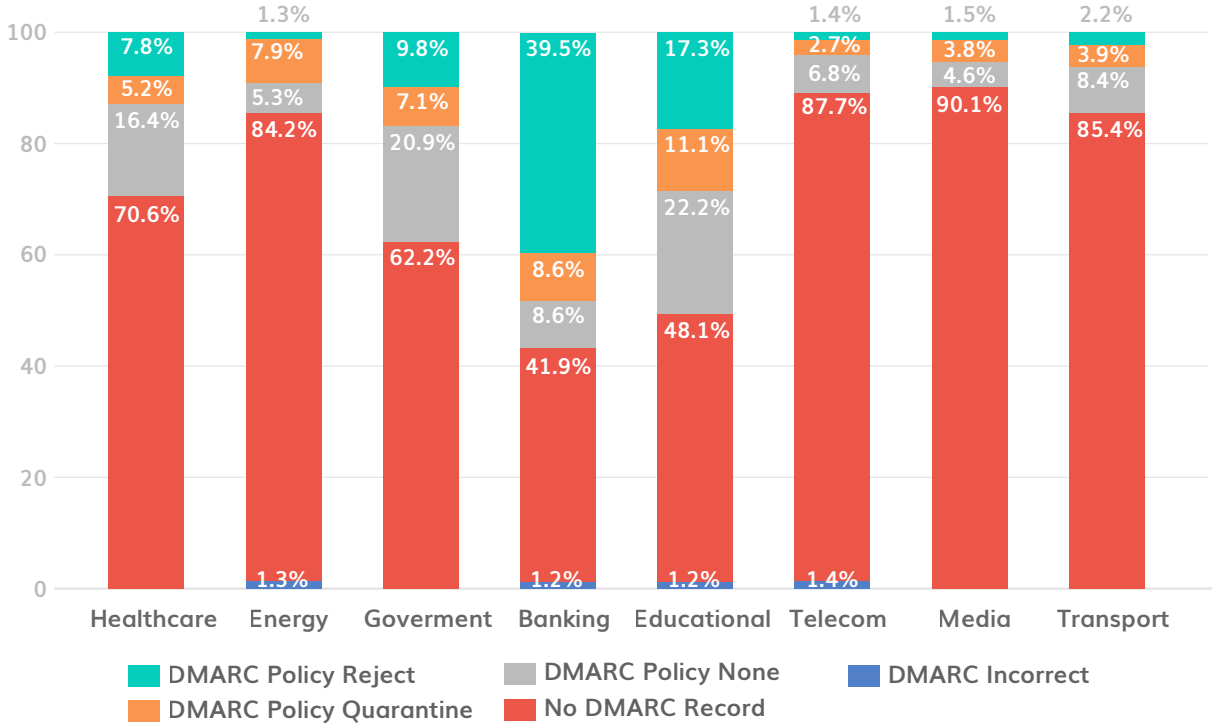
- 25.3% of domains had no SPF record
- 8.4% of the domains had their DMARC policy set at p=none
- No DMARC record was found for 85.4% of the domains

Comparative Analysis of SPF Adoption among Different Sectors in the UAE



The SPF adoption rate was found to be **low** in the UAE **Media and Telecom sectors.** The **highest** rate of SPF adoption was noted in the UAE **Government sector.**

Comparative Analysis of DMARC Adoption among Different Sectors in the UAE



The UAE **Banking, Education and Telecom sectors** noted **low rates** of DMARC adoption. The **highest rate** of DMARC adoption was noted among **Government institutions** in the UAE. A large percentage of organizations in all sectors had their DMARC policies at **monitoring only.**

Critical Errors Organizations in Saudi Arabia are Making

On analyzing 961 UAE domains from various sectors and industries, it is evident that organizations in the UAE are making some critical errors that can jeopardize their online reputation and the safety of their clients:

Incorrect SPF records

Having incorrect SPF records can cause issues with email delivery, as recipient mail servers may mark emails as spam or reject them, resulting in delivery problems. This can have a negative impact on the sender's email reputation if a significant number of emails are marked as spam or rejected. Additionally, incorrect SPF records can make emails vulnerable to phishing attacks and other types of email fraud, as proper authentication is prevented. When emails from a sender with an incorrect SPF record are marked as spam, it can also cause confusion among recipients about the sender's identity, which can damage their credibility.

To avoid these issues, it is crucial to have a well-configured and up-to-date SPF record to ensure that emails sent from your domain are properly authenticated and delivered to their intended recipients.

Low SPF and DMARC adoption rates

A significant portion of domains do not have SPF and DMARC records, which are crucial industry standards for protecting your domain against unauthorized use, reducing the risk of spoofing, phishing, and BEC, and serving as the initial defense against ransomware attacks. It is essential to have these records in place to ensure that your domain is adequately protected and that potential cyber threats are mitigated. By implementing SPF and DMARC records, you can significantly improve the security of your domain and protect against various forms of malicious activity.

DMARC policy lacking enforcement

DMARC is an essential tool for protecting against phishing and spoofing attacks, which involve the use of fraudulent or misleading email addresses to deceive recipients into divulging sensitive information. By enforcing DMARC policies such as "quarantine" or "reject," domain owners can significantly reduce the likelihood of these types of attacks succeeding. Without DMARC enforcement, cyber attackers can more easily impersonate legitimate domains and trick recipients into falling for their scams.

When starting with DMARC, using the "none" policy can be a good way to monitor compliance without worrying about email deliverability issues. However, it is important to note that the "none" policy does not provide any protection against attacks. It is essential to eventually move to an enforced policy to ensure that your domain is adequately protected against phishing and spoofing attempts. By implementing DMARC correctly, you can improve the security of your domain and protect against various forms of malicious activity.

Lack of MTA-STS implementation

The email authentication protocol known as MTA-STS ensures that SMTP emails are transmitted through TLS-encrypted channels, thereby preventing man-in-the-middle attacks such as DNS spoofing. By implementing MTA-STS, domain owners can enhance the security of their email systems. However, most UAE domains currently lack MTA-STS, making them vulnerable to exploitation.

Too many DNS lookups for SPF

According to RFC standards, SPF has a maximum limit of 10 DNS lookups. If this limit is exceeded, it can cause SPF to fail and result in false negatives during authentication. A significant percentage of UAE domains were found to have invalid SPF records, likely due to exceeding the DNS lookup limit.

Multiple SPF records for the same domain

Having multiple SPF records for a single domain can also render the SPF invalid. The analysis of the domains revealed that some of them had multiple SPF records for the same domain, which is not considered valid. To ensure the validity of SPF, it is recommended to have only one SPF record per domain.

Steps to be Taken for Improving Email Security in the UAE

- The following steps can be taken by the UAE organizations to improve their overall email security posture:

1. Staying under the 10 DNS lookup limit for SPF
2. Having error-free SPF and DMARC records
3. Having a single SPF/DMARC record per domain
4. Implementing additional layers of security like BIMI, MTA-STS, and TLS-RPT
5. Enabling DMARC RUA and RUF reports for monitoring domains and sending sources
6. Shifting from p=none to p=reject DMARC policy for protection against email-based attacks

How can PowerDMARC Help You in this Process?

Enabling DMARC, DKIM, and SPF in all gateways throughout a company is crucial to achieving a secure email ecosystem. It is important that all components of the company adhere to the same set of security standards to effectively identify and prevent accidental or malicious email sources. PowerDMARC offers a comprehensive range of email security services and hosted solutions to safeguard your brand reputation and customers against various email-related threats.

- **Configuration:** We help you configure your SPF, DKIM, and DMARC records, to ensure that they are valid and error-free through hosted services.
- **Setup:** As soon as you sign up for our DMARC trial we help you set up your DMARC dashboard, and you gain visibility within 72 hours.
- **Monitoring:** We monitor security incidents in email traffic 24X7 and control legitimate sending sources with alerts, reporting, and responsive actions.
- **Reporting:** Daily Aggregate (RUA) and Forensic (RUF) reports help you keep track of all emails that are passing and failing DMARC from your domains.
- **Enforcement:** We help you shift to DMARC enforcement (p=reject/quarantine) safely, and in record time.
- **PowerSPF:** We allow you to always stay under the 10 DNS lookup limit and update on any changes made by your ESPs in real time.
- **Latest Authentication Protocols:** We use the latest email authentication techniques such as MTA-STS, TLS-RPT, and BIMI, along with the standard protocols, to effectively mitigate all impending challenges in email security and authentication.
- **Managed Security Services:** MSP/MSSP-ready platform with a dedicated service desk to support your company's DMARC implementation efforts and to monitor the email authentication health of your domain and the safety of your users.

Let's join hands to increase the rate of DMARC adoption and strengthen the email security infrastructure in businesses across the UAE. Get in touch with us at **support@powerdmarc.com** to find out how we can help protect your domain and business today!

Contact us!